UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/582,143	03/27/2007	Martin Paul Moshal	06-408	8831

20306 7590 07/30/2010

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER	
MYHR, JUSTIN L	

ART UNIT	PAPER NUMBER
3714	

MAIL DATE	DELIVERY MODE
07/30/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/582,143	MOSHAL, MARTIN PAUL	
	Examiner	Art Unit	
	JUSTIN MYHR	3714	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 April 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-88* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-88* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/14/2010*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This office action is in response to amendments filed on 4/14/2010.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claim(s) 18-23, 44-51, and 76-88 are rejected under 35 USC 101 as being directed to non-statutory subject matter because these are method or process claims that do not transform underlying subject matter (such as an article or materials) to a different state or thing, nor are they tied to another statutory class (such as a particular machine). See Diamond v. Diehr, 450 U.S. 175, 184 (1981) (quoting Benson, 409 U.S. at 70); Parker v. Flook, 437 U.S. 584, 588 n.9 (1978) (citing Cochrane v. Deener, 94 U.S. 780, 787-88 (1876)). See also In re Bilski (Fed Cir, 2007-1130, 10/30/2008) where the Fed. Cir. held that method claims must pass the "machine-or-transformation test" in order to be eligible for patent protection under 35 USC 101. Examiner recommends applicant include in the software method claims a processor or controller configured to perform the method steps stored as computer readable instructions on a "non-transitory" computer readable medium.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

6. Claims 1-18, 21-25, 28-45, and 48-88 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hashimoto et al. (US Pub. No. 2002/0053024 A1 hereinafter referred to as Hashimoto) in view of Nguyen et al. (US Pub. No. 2002/0116615 A1 hereinafter referred to as Nguyen) in view of Borgelt eta l. (US Pat. No. 5,398,285 hereinafter referred to as Borgelt).

As per claim 1, Hashimoto teaches a processor module for a user station operable by a user, comprising: a processor (Fig. 14, item 103); a storage memory accessible by the processor (paragraph [0023] memory must be present to store software); an interface facility communicable with the processor and with at least one peripheral device (standard computer has multiple peripheral devices); a unique identification code associated with the processor module (paragraphs [0015] and [0023] public and secret key); and a security module co-operable with the processor, the security module being arranged to decrypt an encrypted software program, to enable execution of the software program by the processor when the program is encrypted with

the unique identification code associated with the processor module, and to disable execution of the software when the software program is encrypted with a code that is different from the unique identification code associated with the processor module (paragraphs [0015] and [0023] the system will not be able to decrypt the program when it is encrypted with another key not associated with the terminal therefore the system will not be able to run it unless the key used to encrypt the program matches the unique code of the machine). Hashimoto does not specifically teach that the software and the user machine are related to a gaming function nor does Hashimoto teach recovering a unique identification code from the encrypted software program and only executing the game when the recovered code matches the unique identification code associated with the processor module. However, Nguyen teaches providing a secure system for the purpose of downloading a game program from a first machine to a second machine for the purpose of the second machine running the game (abstract and Fig. 14) and Borgelt teaches a system in which a unique identification code associated with a first system is sent to a software distributor, encrypted in a return message with a software code, decrypted by a receiving first system, and confirming that the unique identifier received matches the unique identifier of the system before executing the program using the software code (Figs. 1-2, items 101, 107, 200, 202, 204, 205, and 206 and col. 2, lines 50-58). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen and Borgelt, since Hashimoto is modifiable to be used for the gaming art since it is desired in the gaming art to provide a secure and easy manner of downloading and installing

games on a gaming machine (Nguyen paragraph [0016]). In addition, by modifying Hashimoto to include the steps of Borgelt in which the returned encrypted software data (which it would be clear to one of ordinary skill in the art could obviously include the software program as well) includes the unique identifier of the machine requesting the software program and requires the recovered identifier and the machine identifier to match will insure that even in the case where the software date is decrypted using another machine's identifier the receiving machine will still not execute the software unless the identifier matches the receiving machine (see Borgelt col. 1, lines 60 to col. 2, line 11).

As per claim 2, Hashimoto does not specifically teach a processor in which the security module also disables execution of the software program when the software program is unencrypted. However, Hashimoto does teach insuring that illegal analysis and tampering of programs does not occur by use of software encryption (paragraphs [0007]-[0008]). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Hashimoto to prevent software unencrypted from running since the purpose of Hashimoto is to have a processor which processes encrypted software in order to prevent illegal use and this purpose is not fulfilled if the software is not encrypted.

As per claim 3, Hashimoto teaches a processor in which the unique identification code is stored in a protected area of the storage memory (paragraphs [0087]-[0088]).

As per claim 4, Hashimoto does not specifically teach a processor in which the protected area of the storage memory is a read-only memory. However, it would have

been obvious to one of ordinary skill in the art at the time the invention was made to have made the memory read-only since overwriting of the key with a new key would negate the benefit of the described system of Hashimoto since the key is suppose to be unique to each processor (paragraph [0015]).

As per claim 5, Hashimoto teaches a processor in which the interface facility is an input/output circuit connected to the processor by means of an input/output bus (Fig. 1, items 103 and 105).

As per claim 6, Hashimoto teaches a processor in which the at least one peripheral device is any one of a display monitor, a magnetic card reader, a banknote validator, an array of pushbuttons, a coin acceptor, a ticket reader, a numeric keypad, a printer and a counter (well known that computers include a monitor).

As per claim 7, Hashimoto does not specifically teach a processor in which communication between the processor and the at least one peripheral device is encrypted. However, it is old and well known in the art at the time the invention was made to encrypt the communication between peripheral devices for security purposes.

As per claims 8 and 9, Hashimoto does not teach a processor in which the processor module includes a hardware random number generator. However, it is old and well known in the art at the time the invention was made to include hardware based random number generators in order to produce random outcomes.

As per claims 10 and 11, Hashimoto does not specifically teach a processor in which the storage memory includes a still further portion that is removable. However, it

is well known in the art at the time the invention was made that computers include removable storage medium including USB devices, disks, and flash drives.

As per claim 12, Hashimoto teaches a processor in which the processor includes a network interface that provides access to a communication network (Fig. 1, items 103 and 105).

As per claim 13, Hashimoto teaches a processor in which the communication network is the Internet (paragraph [0052]).

As per claim 14, Hashimoto teaches a processor in which the processor module also includes a number of interface ports (well known feature in computers).

As per claim 15, Hashimoto does not specifically teach a processor in which the number of interface ports include any one or more of a serial communication port and a port conforming to the Universal Serial Bus standard. However, this is a well known feature in computers. Hence, it would have been obvious to one of ordinary skill in the art that Hashimoto could include USB ports as found in the average user computer.

As per claim 16, Hashimoto teaches a method for configuring a processor module for a user station operable by a user, comprising the steps of: providing a software program executable by the processor module (abstract); obtaining a unique identification code associated with the processor module (paragraphs [0015] and [0023]); encrypting the software program remotely from the processor module as a function of the unique identification code (paragraph [0023]); transferring the encrypted software program to the processor module (paragraph [0023]); and decrypting the encrypted software program (paragraph [0023]), and enabling execution of the

encrypted software program by the processor when the program is encrypted with the unique identification code associated with the processor module, and to disable execution of the software when the software program is encrypted with a code that is different from the unique identification code associated with the processor module (paragraphs [0015] and [0023] the system will not be able to decrypt the program when it is encrypted with another key not associated with the terminal therefore the system will not be able to run it unless the key used to encrypt the program matches the unique code of the machine). Hashimoto does not specifically teach that the software and the user machine are related to a gaming function nor does Hashimoto teach recovering a unique identification code from the encrypted software program and only executing the game when the recovered code matches the unique identification code associated with the processor module. However, Nguyen teaches providing a secure system for the purpose of downloading a game program from a first machine to a second machine for the purpose of the second machine running the game (abstract and Fig. 14) and Borgelt teaches a system in which a unique identification code associated with a first system is sent to a software distributor, encrypted in a return message with a software code, decrypted by a receiving first system, and confirming that the unique identifier received matches the unique identifier of the system before executing the program using the software code (Figs. 1-2, items 101, 107, 200, 202, 204, 205, and 206 and col. 2, lines 50-58). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen and Borgelt, since Hashimoto is modifiable to be used for the gaming art since it is desired

in the gaming art to provide a secure and easy manner of downloading and installing games on a gaming machine (Nguyen paragraph [0016]). In addition, by modifying Hashimoto to include the steps of Borgelt in which the returned encrypted software data (which it would be clear to one of ordinary skill in the art could obviously include the software program as well) includes the unique identifier of the machine requesting the software program and requires the recovered identifier and the machine identifier to match will insure that even in the case where the software date is decrypted using another machine's identifier the receiving machine will still not execute the software unless the identifier matches the receiving machine (see Borgelt col. 1, lines 60 to col. 2, line 11).

As per claim 17, Hashimoto does not specifically teach a method in which the security module also disables execution of the software program when the software program is unencrypted. However, Hashimoto does teach insuring that illegal analysis and tampering of programs does not occur by use of software encryption (paragraphs [0007]-[0008]). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Hashimoto to prevent software unencrypted from running since the purpose of Hashimoto is to have a processor which processes encrypted software in order to prevent illegal use and this purpose is not fulfilled if the software is not encrypted.

As per claim 18, Hashimoto teaches a method in which the unique identification code is stored in a protected area of the storage memory associated with the processor module (paragraphs [0087]-[0088]).

As per claim 21, Hashimoto teaches a method that includes a step of jointly encrypting a plurality of different software programs remotely from the processor module as a function of the unique identification code, each one of the plurality of software programs being executable to produce a simulation of a different game (it is clear that a user can purchase multiple software programs in Hashimoto and not just one).

As per claim 22, Hashimoto teaches a method in which the jointly encrypted plurality of software programs are transferred to the processor module (paragraph [0023]).

As per claim 23, Hashimoto does not specifically teach a method in which the jointly encrypted plurality of software programs are decrypted to obtain a decrypted identification code therefrom, and execution of any selected one of the jointly encrypted plurality of software programs is enabled when the decrypted identification code is the same as the unique identification code of the processor module, and execution of all of the jointly encrypted plurality of software programs is disabled when the decrypted identification code is different from the unique identification code of the processor module. However, Borgelt teaches a system in which a unique identification code associated with a first system is sent to a software distributor, encrypted in a return message with a software code, decrypted by a receiving first system, and confirming that the unique identifier received matches the unique identifier of the system before executing the program using the software code (Figs. 1-2, items 101, 107, 200, 202, 204, 205, and 206 and col. 2, lines 50-58). Hence, it would have been obvious to one of

ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen and Borgelt, since it is clear that a user can purchase multiple software programs in Hashimoto and not just one. In addition, by modifying Hashimoto to include the steps of Borgelt in which the returned encrypted software data (which it would be clear to one of ordinary skill in the art could obviously include the software program as well) includes the unique identifier of the machine requesting the software program and requires the recovered identifier and the machine identifier to match will insure that even in the case where the software date is decrypted using another machine's identifier the receiving machine will still not execute the software unless the identifier matches the receiving machine (see Borgelt col. 1, lines 60 to col. 2, line 11).

As per claim 24, Hashimoto teaches a system for customization and distribution of software, comprising: a number of user stations, each user station being operable by a respective user to use a corresponding program, each user station being associated with a unique identification code (paragraphs [0015] and [0023]); a repository containing a number of different software programs, each software program being executable by at least one of the number of user stations (Fig. 1, items 101 and 102); a download server communicable with the repository (Fig. 1, item 102); a communication network enabling communication between the download server and each one of the number of user stations (Fig. 1, item 105); encryption means operable to encrypt, remotely from the number of user stations, a selectable one of the number of different software programs contained in the repository as a function of the unique identification code of a selectable

one of the number of user stations, the download server being responsive to the encryption means to download the encrypted software program to the particular user station whose unique identification code was used for encryption (paragraphs [0015] and [0023]); and a security module associated with the particular user station, the security module being capable of decrypting the downloaded encrypted software program (paragraph [0023]) and enabling execution of the software program by the processor when the program is encrypted with the unique identification code associated with the processor module, and to disable execution of the software when the software program is encrypted with a code that is different from the unique identification code associated with the processor module (paragraphs [0015] and [0023] the system will not be able to decrypt the program when it is encrypted with another key not associated with the terminal therefore the system will not be able to run it unless the key used to encrypt the program matches the unique code of the machine). Hashimoto does not specifically teach that the software and the user machine are related to a gaming function nor does Hashimoto teach recovering a unique identification code from the encrypted software program and only executing the game when the recovered code matches the unique identification code associated with the processor module. However, Nguyen teaches providing a secure system for the purpose of downloading a game program from a first machine to a second machine for the purpose of the second machine running the game (abstract and Fig. 14) and Borgelt teaches a system in which a unique identification code associated with a first system is sent to a software distributor, encrypted in a return message with a software code, decrypted by a

receiving first system, and confirming that the unique identifier received matches the unique identifier of the system before executing the program using the software code (Figs. 1-2, items 101, 107, 200, 202, 204, 205, and 206 and col. 2, lines 50-58). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen and Borgelt, since Hashimoto is modifiable to be used for the gaming art since it is desired in the gaming art to provide a secure and easy manner of downloading and installing games on a gaming machine (Nguyen paragraph [0016]). In addition, by modifying Hashimoto to include the steps of Borgelt in which the returned encrypted software data (which it would be clear to one of ordinary skill in the art could obviously include the software program as well) includes the unique identifier of the machine requesting the software program and requires the recovered identifier and the machine identifier to match will insure that even in the case where the software date is decrypted using another machine's identifier the receiving machine will still not execute the software unless the identifier matches the receiving machine (see Borgelt col. 1, lines 60 to col. 2, line 11).

As per claim 25, Hashimoto does not specifically teach a system in which the security module also disables execution of the software program when the software program is unencrypted. However, Hashimoto does teach insuring that illegal analysis and tampering of programs does not occur by use of software encryption (paragraphs [0007]-[0008]). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Hashimoto to prevent software unencrypted from running since the purpose of Hashimoto is to have a processor which

processes encrypted software in order to prevent illegal use and this purpose is not fulfilled if the software is not encrypted.

As per claim 28, Hashimoto teaches a system that includes a step of jointly encrypting a plurality of different software programs remotely from the processor module as a function of the unique identification code, each one of the plurality of software programs being executable to produce a simulation of a different game (it is clear that a user can purchase multiple software programs in Hashimoto and not just one).

As per claim 29, Hashimoto teaches a system in which the download server is responsive to the encryption means to download the encrypted plurality of software programs are transferred to the processor module (paragraph [0023]).

As per claim 30, Hashimoto does not specifically teach a system in which the security module decrypts the jointly encrypted plurality of software programs are decrypted to obtain a decrypted identification code therefrom, and execution of any selected one of the jointly encrypted plurality of software- programs is enabled when the decrypted identification code is the same as the unique identification code of the processor module, and execution of all of the jointly encrypted plurality of software programs is disabled when the decrypted identification code is different from the unique identification code of the processor module. However, Borgelt teaches a system in which a unique identification code associated with a first system is sent to a software distributor, encrypted in a return message with a software code, decrypted by a receiving first system, and confirming that the unique identifier received matches the

unique identifier of the system before executing the program using the software code (Figs. 1-2, items 101, 107, 200, 202, 204, 205, and 206 and col. 2, lines 50-58). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen and Borgelt, since it is clear that a user can purchase multiple software programs in Hashimoto and not just one. In addition, by modifying Hashimoto to include the steps of Borgelt in which the returned encrypted software data (which it would be clear to one of ordinary skill in the art could obviously include the software program as well) includes the unique identifier of the machine requesting the software program and requires the recovered identifier and the machine identifier to match will insure that even in the case where the software date is decrypted using another machine's identifier the receiving machine will still not execute the software unless the identifier matches the receiving machine (see Borgelt col. 1, lines 60 to col. 2, line 11).

As per claim 31, Hashimoto teaches a system in which each player station has an associated storage memory (paragraph [0023]).

As per claim 32, Hashimoto teaches a system in which the unique identification code is stored in a protected area of the storage memory (paragraphs [0087]-[0088]).

As per claim 33, Hashimoto does not specifically teach a system in which the protected area of the storage memory is a read-only memory. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have made the memory read-only since overwriting of the key with a new key would

negate the benefit of the described system of Hashimoto since the key is suppose to be unique to each processor (paragraph [0015]).

As per claim 34, Hashimoto teaches a system in which each player station includes a processor and a number of peripheral devices (Hashimoto teaches a computer which it is well knows includes a processor and a number of attached devices).

As per claim 35, Hashimoto teaches a system in which the at least one peripheral device is any one of a display monitor, a magnetic card reader, a banknote validator, an array of pushbuttons, a coin acceptor, a ticket reader, a numeric keypad, a printer and a counter (well known that computers include a monitor).

As per claim 36, Hashimoto does not specifically teach a system in which communication between the processor and the at least one peripheral device is encrypted. However, it is old and well known in the art at the time the invention was made to encrypt the communication between peripheral devices for security purposes.

As per claims 37 and 38, Hashimoto does not teach a system in which the processor module includes a hardware random number generator. However, it is old and well known in the art at the time the invention was made to include hardware based random number generators in order to produce random outcomes.

As per claims 39 and 40, Hashimoto does not specifically teach a system in which the storage memory includes a still further portion that is removable. However, it is well known in the art at the time the invention was made that computers include removable storage medium including USB devices, disks, and flash drives.

As per claim 41, Hashimoto teaches a system in which the communication network is the Internet (paragraph [0052]).

As per claim 42, Hashimoto teaches a processor in which the system module also includes a number of interface ports (well known feature in computers).

As per claim 43, Hashimoto does not specifically teach a system in which the number of interface ports include any one or more of a serial communication port and a port conforming to the Universal Serial Bus standard. However, this is a well known feature in computers. Hence, it would have been obvious to one of ordinary skill in the art that Hashimoto could include USB ports as found in the average user computer.

As per claim 44, Hashimoto teaches a method for the customization and distribution of software, comprising the steps of: providing a number of user stations, each user station being operable by a respective player for use, each user station being associated with a unique identification code (paragraphs [0015] and [0023]); providing a repository containing a number of different software programs, each software program being executable by at least one of the number of user stations (Fig. 1, items 101 and 102); encrypting, remotely from the number of player stations, a selected one of the number of different software programs contained in the repository as a function of the unique identification code of a selected one of the number of player stations; downloading the encrypted software program to the particular user station whose unique identification code was used for encryption (paragraphs [0015] and [0023]); decrypting the downloaded encrypted software program (paragraph [0023]); and enabling execution of the software program by the processor when the program is

encrypted with the unique identification code associated with the processor module, and to disable execution of the software when the software program is encrypted with a code that is different from the unique identification code associated with the processor module (paragraphs [0015] and [0023] the system will not be able to decrypt the program when it is encrypted with another key not associated with the terminal therefore the system will not be able to run it unless the key used to encrypt the program matches the unique code of the machine). Hashimoto does not specifically teach that the software and the user machine are related to a gaming function nor does Hashimoto teach recovering a unique identification code from the encrypted software program and only executing the game when the recovered code matches the unique identification code associated with the processor module. However, Nguyen teaches providing a secure system for the purpose of downloading a game program from a first machine to a second machine for the purpose of the second machine running the game (abstract and Fig. 14) and Borgelt teaches a system in which a unique identification code associated with a first system is sent to a software distributor, encrypted in a return message with a software code, decrypted by a receiving first system, and confirming that the unique identifier received matches the unique identifier of the system before executing the program using the software code (Figs. 1-2, items 101, 107, 200, 202, 204, 205, and 206 and col. 2, lines 50-58). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen and Borgelt, since Hashimoto is modifiable to be used for the gaming art since it is desired in the gaming art to provide a secure and

easy manner of downloading and installing games on a gaming machine (Nguyen paragraph [0016]). In addition, by modifying Hashimoto to include the steps of Borgelt in which the returned encrypted software data (which it would be clear to one of ordinary skill in the art could obviously include the software program as well) includes the unique identifier of the machine requesting the software program and requires the recovered identifier and the machine identifier to match will insure that even in the case where the software date is decrypted using another machine's identifier the receiving machine will still not execute the software unless the identifier matches the receiving machine (see Borgelt col. 1, lines 60 to col. 2, line 11).

As per claim 45, Hashimoto does not specifically teach a method in which the security module also disables execution of the software program when the software program is unencrypted. However, Hashimoto does teach insuring that illegal analysis and tampering of programs does not occur by use of software encryption (paragraphs [0007]-[0008]). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Hashimoto to prevent software unencrypted from running since the purpose of Hashimoto is to have a processor which processes encrypted software in order to prevent illegal use and this purpose is not fulfilled if the software is not encrypted.

As per claim 48, Hashimoto teaches a method that includes a step of jointly encrypting a plurality of different software programs remotely from the processor module as a function of the unique identification code, each one of the plurality of software programs being executable to produce a simulation of a different game (it is

clear that a user can purchase multiple software programs in Hashimoto and not just one).

As per claim 49, Hashimoto teaches a method in which the jointly encrypted plurality of software programs are downloaded to the particular player station whose unique identification code was used for encryption (paragraph [0023]).

As per claim 50, Hashimoto does not specifically teach a method in which jointly encrypted plurality of software programs are decrypted to obtain a decrypted identification code therefrom, and execution of any selected one of the jointly encrypted plurality of software- programs is enabled when the decrypted identification code is the same as the unique identification code of the processor module, and execution of all of the jointly encrypted plurality of software programs is disabled when the decrypted identification code is different from the unique identification code of the processor module. However, Borgelt teaches a system in which a unique identification code associated with a first system is sent to a software distributor, encrypted in a return message with a software code, decrypted by a receiving first system, and confirming that the unique identifier received matches the unique identifier of the system before executing the program using the software code (Figs. 1-2, items 101, 107, 200, 202, 204, 205, and 206 and col. 2, lines 50-58). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen and Borgelt, since it is clear that a user can purchase multiple software programs in Hashimoto and not just one. In addition, by modifying Hashimoto to include the steps of Borgelt in which the returned encrypted

software data (which it would be clear to one of ordinary skill in the art could obviously include the software program as well) includes the unique identifier of the machine requesting the software program and requires the recovered identifier and the machine identifier to match will insure that even in the case where the software date is decrypted using another machine's identifier the receiving machine will still not execute the software unless the identifier matches the receiving machine (see Borgelt col. 1, lines 60 to col. 2, line 11).

As per claim 51, Hashimoto teaches a method in which the unique identification code is stored in a protected area of the storage memory (paragraphs [0087]-[0088]).

As per claim 52, Hashimoto teaches a system for the distribution of software, comprising: a repository containing a number of different software programs (Fig. 1, items 101 and 102); a number of processor modules, each processor module being identified by means of a unique identification code and being operable to execute any one of the number of different software programs contained in the repository (Fig. 1, item 103 and paragraphs [0015] and [0023]); encryption means operable to encrypt, remotely from the number of user stations, a selectable one of the number of different software programs contained in the repository as a function of the unique identification code of a selectable one of the number of user stations (paragraphs [0015] and [0023]); a download facility operable to download the encrypted particular software program to the particular processor module whose identification code was used for encryption (paragraph [0023]); and a security module associated with the particular user station, the security module being capable of decrypting the downloaded encrypted software

program (paragraph [0023]) and enabling execution of the software program by the processor when the program is encrypted with the unique identification code associated with the processor module, and to disable execution of the software when the software program is encrypted with a code that is different from the unique identification code associated with the processor module (paragraphs [0015] and [0023] the system will not be able to decrypt the program when it is encrypted with another key not associated with the terminal therefore the system will not be able to run it unless the key used to encrypt the program matches the unique code of the machine). Hashimoto does not specifically teach that the software and the user machine are related to a gaming function nor does Hashimoto teach recovering a unique identification code from the encrypted software program and only executing the game when the recovered code matches the unique identification code associated with the processor module. In addition, though Hashimoto teaches charging for the distributed software (paragraph [0107]) it does not specifically teach receiving means for receiving a request for a license to execute a desired combination of at least one software program contained in the repository on at least one of the number of processor modules, the license request containing at least one selectable identification code-to-software program mapping and payment means for receiving a fee for the requested license. However, Nguyen teaches providing a secure system for the purpose of downloading a game program from a first machine to a second machine for the purpose of the second machine running the game (abstract and Fig. 14) and obtaining a license on a gaming machine for a purchase piece of software (Figs. 6 and 7) and Borgelt teaches a system in which

a unique identification code associated with a first system is sent to a software distributor, encrypted in a return message with a software code, decrypted by a receiving first system, and confirming that the unique identifier received matches the unique identifier of the system before executing the program using the software code (Figs. 1-2, items 101, 107, 200, 202, 204, 205, and 206 and col. 2, lines 50-58). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen and Borgelt, since Hashimoto is modifiable to be used for the gaming art since it is desired in the gaming art to provide a secure and easy manner of downloading and installing games on a gaming machine (Nguyen paragraph [0016]) and obtaining the needed license in order to operate the software on the gaming machine. In addition, by modifying Hashimoto to include the steps of Borgelt in which the returned encrypted software data (which it would be clear to one of ordinary skill in the art could obviously include the software program as well) includes the unique identifier of the machine requesting the software program and requires the recovered identifier and the machine identifier to match will insure that even in the case where the software date is decrypted using another machine's identifier the receiving machine will still not execute the software unless the identifier matches the receiving machine (see Borgelt col. 1, lines 60 to col. 2, line 11).

As per claim 53, Hashimoto does not specifically teach a system in which the at least one selectable mapping is a one-to-one mapping. However, Nguyen does teach a system in which the at least one selectable mapping is a one-to-one mapping

(paragraph [0099]). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen and Borgelt, since Hashimoto is modifiable to allow the purchase of licenses which enable a single gaming machine to run the downloaded game thereby saving the operator time since they do not need to go through the hassle of purchasing the license separately.

As per claim 54, Hashimoto does not specifically teach a system in which the license request contains a plurality of different one-to-one mappings, each unique processor module identification code being contained in only one such mapping. However, Nguyen does teach a system in which the license request contains a plurality of different one-to-one mappings, each unique processor module identification code being contained in only one such mapping (Figs. 6-7 and paragraph [0099] able to purchase multiple licenses depending on need). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen and Borgelt, since Hashimoto is modifiable to allow the purchase of licenses which enable a single gaming machine to run the downloaded game thereby saving the operator time since they do not need to go through the hassle of purchasing the license separately.

As per claim 55, Hashimoto does not specifically teach a system in which the encryption means is responsive to payment of the fee to encrypt the particular software program contained in each one of the plurality of different one-to-one mappings as a function of the identification code in that mapping. However, it would have been

obvious to one of ordinary skill in the art that Hashimoto would require the software to be purchased first before allowing a user to download it since the key needed to decrypt the software is already present on the system.

As per claim 56, Hashimoto teaches a system in which the download facility downloads each encrypted software program to the particular processor module whose identification code was used for encryption (paragraph [0023]).

As per claim 57, Hashimoto does not specifically teach a system in which the at least one selectable mapping is a many-to-one mapping. However, Nguyen does teach a system in which the at least one selectable mapping is a many-to-one mapping (Figs. 6-7 and paragraph [0078] can purchase a license for multiple games and paragraph [0133] allows for multiple gaming machines per license). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen and Borgelt, since Hashimoto is modifiable to allow the purchase of licenses which enable a single gaming machine to run the downloaded game thereby saving the operator time since they do not need to go through the hassle of purchasing the license separately.

As per claim 58, Hashimoto does not specifically teach a system each unique processor module identification code being contained in only one such mapping. However, Nguyen does teach a system in which the at least one selectable mapping is a many-to-one mapping (Figs. 6-7 and paragraph [0078] can purchase a license for multiple games and paragraph [0133] allows for multiple gaming machines per license) and Hashimoto teaches encrypting the download using the gaming machines unique

code in every download (paragraph [0023]). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen and Borgelt, since Hashimoto is modifiable to allow the purchase of licenses which enable a single gaming machine to run the downloaded game thereby saving the operator time since they do not need to go through the hassle of purchasing the license separately.

As per claim 59, Hashimoto does not specifically teach a system in which the encryption means is responsive to payment of the fee to encrypt the particular software program contained in each one of the different many-to-one mappings with each one of the plurality of identification codes in that mapping to obtain separate encrypted instances of the same software program. However, it would have been obvious to one of ordinary skill in the art that Hashimoto would require the software to be purchased first before allowing a user to download it since the key needed to decrypt the software is already present on the system.

As per claim 60, Hashimoto teaches a system in which the download facility downloads each encrypted software program to the particular processor module whose identification code was used for encryption (paragraph [0023]).

As per claim 61, Hashimoto does not specifically teach a system in which the security module also disables execution of the software program when the software program is unencrypted. However, Hashimoto does teach insuring that illegal analysis and tampering of programs does not occur by use of software encryption (paragraphs [0007]-[0008]). Hence, it would have been obvious to one of ordinary skill in the art at

the time the invention was made to have modified Hashimoto to prevent software unencrypted from running since the purpose of Hashimoto is to have a processor which processes encrypted software in order to prevent illegal use and this purpose is not fulfilled if the software is not encrypted.

As per claim 62, Hashimoto teaches a system in which each processor module has an associated storage memory (paragraphs [0087]-[0088]).

As per claim 63, Hashimoto teaches a system in which the unique identification code is stored in a protected area of the storage memory (paragraphs [0087]-[0088]).

As per claim 64, Hashimoto does not specifically teach a system in which the protected area of the storage memory is a read-only memory. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have made the memory read-only since overwriting of the key with a new key would negate the benefit of the described system of Hashimoto since the key is suppose to be unique to each processor (paragraph [0015]).

As per claim 65, Hashimoto teaches a system in which the processor module is interfaceable to at least one peripheral device (well known that computers include a monitor).

As per claim 66, Hashimoto teaches a system in which the at least one peripheral device is any one of a display monitor, a magnetic card reader, a banknote validator, an array of pushbuttons, a coin acceptor, a ticket reader, a numeric keypad, a printer and a counter (well known that computers include a monitor).

As per claim 67, Hashimoto does not specifically teach a system in which communication between the processor and the at least one peripheral device is encrypted. However, it is old and well known in the art at the time the invention was made to encrypt the communication between peripheral devices for security purposes.

As per claims 68 and 69, Hashimoto does not teach a system in which the processor module includes a hardware random number generator. However, it is old and well known in the art at the time the invention was made to include hardware based random number generators in order to produce random outcomes.

As per claims 70 and 71, Hashimoto does not specifically teach a system in which the storage memory includes a still further portion that is removable. However, it is well known in the art at the time the invention was made that computers include removable storage medium including USB devices, disks, and flash drives.

As per claim 72, Hashimoto teaches a system in which the processor includes a network interface that provides access to a communication network (Fig. 1, items 103 and 105).

As per claim 73, Hashimoto teaches a system in which the communication network is the Internet (paragraph [0052]).

As per claim 74, Hashimoto teaches a system in which the processor module also includes a number of interface ports (well known feature in computers).

As per claim 75, Hashimoto does not specifically teach a system in which the number of interface ports include any one or more of a serial communication port and a port conforming to the Universal Serial Bus standard. However, this is a well known

feature in computers. Hence, it would have been obvious to one of ordinary skill in the art that Hashimoto could include USB ports as found in the average user computer.

As per claim 76, Hashimoto teaches a method for the distribution of software, comprising the steps of: providing a repository containing a number of different software programs, each software program being executable by at least one of the number of user stations (Fig. 1, items 101 and 102); a number of processor modules, each processor module being identified by means of a unique identification code and being operable to execute any one of the number of different software programs contained in the repository (Fig. 1, item 103 and paragraphs [0015] and [0023]); encrypting, remotely from the number of player stations, a selected one of the number of different software programs contained in the repository as a function of the unique identification code of a selected one of the number of player stations; downloading the encrypted software program to the particular user station whose unique identification code was used for encryption (paragraphs [0015] and [0023]); decrypting the downloaded encrypted software program (paragraph [0023]), and enabling execution of the software program by the processor when the program is encrypted with the unique identification code associated with the processor module, and to disable execution of the software when the software program is encrypted with a code that is different from the unique identification code associated with the processor module (paragraphs [0015] and [0023] the system will not be able to decrypt the program when it is encrypted with another key not associated with the terminal therefore the system will not be able to run it unless the key used to encrypt the program matches the unique code of the machine). Hashimoto

does not specifically teach that the software and the user machine are related to a gaming function nor does Hashimoto teach recovering a unique identification code from the encrypted software program and only executing the game when the recovered code matches the unique identification code associated with the processor module. In addition, though Hashimoto teaches charging for the distributed software (paragraph [0107]) it does not specifically teach receiving means for receiving a request for a license to execute a desired combination of at least one software program contained in the repository on at least one of the number of processor modules, the license request containing at least one selectable identification code-to-software program mapping and payment means for receiving a fee for the requested license. However, Nguyen teaches providing a secure system for the purpose of downloading a game program from a first machine to a second machine for the purpose of the second machine running the game (abstract and Fig. 14) and obtaining a license on a gaming machine for a purchase piece of software (Figs. 6 and 7) and Borgelt teaches a system in which a unique identification code associated with a first system is sent to a software distributor, encrypted in a return message with a software code, decrypted by a receiving first system, and confirming that the unique identifier received matches the unique identifier of the system before executing the program using the software code (Figs. 1-2, items 101, 107, 200, 202, 204, 205, and 206 and col. 2, lines 50-58). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen and Borgelt, since Hashimoto is modifiable to be used for the gaming art since it is desired in the

gaming art to provide a secure and easy manner of downloading and installing games on a gaming machine (Nguyen paragraph [0016]) and obtaining the needed license in order to operate the software on the gaming machine. In addition, by modifying Hashimoto to include the steps of Borgelt in which the returned encrypted software data (which it would be clear to one of ordinary skill in the art could obviously include the software program as well) includes the unique identifier of the machine requesting the software program and requires the recovered identifier and the machine identifier to match will insure that even in the case where the software date is decrypted using another machine's identifier the receiving machine will still not execute the software unless the identifier matches the receiving machine (see Borgelt col. 1, lines 60 to col. 2, line 11).

As per claim 77, Hashimoto does not specifically teach a method in which the at least one selectable mapping is a one-to-one mapping. However, Nguyen does teach a system in which the at least one selectable mapping is a one-to-one mapping (paragraph [0099]). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen and Borgelt, since Hashimoto is modifiable to allow the purchase of licenses which enable a single gaming machine to run the downloaded game thereby saving the operator time since they do not need to go through the hassle of purchasing the license separately.

As per claim 78, Hashimoto does not specifically teach a method in which the license request contains a plurality of different one-to-one mappings, each unique

processor module identification code being contained in only one such mapping. However, Nguyen does teach a system in which the license request contains a plurality of different one-to-one mappings, each unique processor module identification code being contained in only one such mapping (Figs. 6-7 and paragraph [0099] able to purchase multiple licenses depending on need). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen and Borgelt, since Hashimoto is modifiable to allow the purchase of licenses which enable a single gaming machine to run the downloaded game thereby saving the operator time since they do not need to go through the hassle of purchasing the license separately.

As per claim 79, Hashimoto does not specifically teach a method in which the encryption means is responsive to payment of the fee to encrypt the particular software program contained in each one of the plurality of different one-to-one mappings as a function of the identification code in that mapping. However, it would have been obvious to one of ordinary skill in the art that Hashimoto would require the software to be purchased first before allowing a user to download it since the key needed to decrypt the software is already present on the system.

As per claim 80, Hashimoto teaches a method in which each encrypted software program is downloaded to the particular processor module whose identification code war, used for encryption (paragraph [0023]).

As per claim 81, Hashimoto does not specifically teach a method in which the at least one selectable mapping is a many-to-one mapping. However, Nguyen does teach

a system in which the at least one selectable mapping is a many-to-one mapping (Figs. 6-7 and paragraph [0078] can purchase a license for multiple games and paragraph [0133] allows for multiple gaming machines per license). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen and Borgelt, since Hashimoto is modifiable to allow the purchase of licenses which enable a single gaming machine to run the downloaded game thereby saving the operator time since they do not need to go through the hassle of purchasing the license separately.

As per claim 82, Hashimoto does not specifically teach a method each unique processor module identification code being contained in only one such mapping. However, Nguyen does teach a system in which the at least one selectable mapping is a many-to-one mapping (Figs. 6-7 and paragraph [0078] can purchase a license for multiple games and paragraph [0133] allows for multiple gaming machines per license) and Hashimoto teaches encrypting the download using the gaming machines unique code in every download (paragraph [0023]). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen and Borgelt, since Hashimoto is modifiable to allow the purchase of licenses which enable a single gaming machine to run the downloaded game thereby saving the operator time since they do not need to go through the hassle of purchasing the license separately.

As per claim 83, Hashimoto does not specifically teach a method in which the encryption means is responsive to payment of the fee to encrypt the particular software

program contained in each one of the different many-to-one mappings with each one of the plurality of identification codes in that mapping to obtain separate encrypted instances of the same software program. However, it would have been obvious to one of ordinary skill in the art that Hashimoto would require the software to be purchased first before allowing a user to download it since the key needed to decrypt the software is already present on the system.

As per claim 84, Hashimoto teaches a method in which each encrypted instance of a software program is downloaded to the particular processor module whose identification code was used for encryption in that instance (paragraph [0023]).

As per claim 85, Hashimoto does not specifically teach a method in which execution of the software program is disabled when the software program is unencrypted. However, Hashimoto does teach insuring that illegal analysis and tampering of programs does not occur by use of software encryption (paragraphs [0007]-[0008]). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Hashimoto to prevent software unencrypted from running since the purpose of Hashimoto is to have a processor which processes encrypted software in order to prevent illegal use and this purpose is not fulfilled if the software is not encrypted.

As per claim 86, Hashimoto teaches a method in which the unique identification code is stored in a protected area of the storage memory (paragraphs [0087]-[0088]).

As per claim 87, Hashimoto teaches a method in which the processor module is interfaceable to at least one peripheral device (well known that computers include a monitor).

As per claim 88, Hashimoto does not specifically teach a method in which communication between the processor and the at least one peripheral device is encrypted. However, it is old and well known in the art at the time the invention was made to encrypt the communication between peripheral devices for security purposes.

7. Claims 19-20, 26-27, and 46-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hashimoto et al. (US Pub. No. 2002/0053024 A1 hereinafter referred to as Hashimoto), Nguyen et al. (US Pub. No. 2002/0116615 A1 hereinafter referred to as Nguyen) and Borgelt et al. (US Pat. No. 5,398,285 hereinafter referred to as Borgelt) in view of Reeder (US Pat. No. 6,141,652).

As per claims 19, 26, and 46, Hashimoto does not specifically teach a method in which execution of the encrypted software program is enabled for a predetermined period of time. However, Reeder does teach a method in which execution of the encrypted software program is enabled for a predetermined period of time (col. 7, lines 16-30 renting software). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen, Borgelt and Reeder, since Hashimoto is modifiable to include support for rentable software in which validation is sought after a set amount of time in order to allow a gaming machine to continue executing the game after confirming with the provider that the copy is still valid.

As per claims 20, 27, and 47, Hashimoto does not specifically teach a method in which execution of the encrypted software program is re-enabled upon the occurrence of a predetermined event. However, Reeder does teach a method in which execution of the encrypted software program is re-enabled upon the occurrence of a predetermined event (col. 7, lines 16-30 renting software). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Hashimoto with Nguyen, Borgelt and Reeder, since Hashimoto is modifiable to include support for rentable software in which validation is sought after a set amount of time in order to allow a gaming machine to continue executing the game after confirming with the provider that the copy is still valid.

Response to Arguments

8. Applicant's arguments with respect to claims 1-88 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Shimada et al. (US Pub. No. 2003/0123670 A1) teaches a system in which at least some identification information is sent to a program distributor after a system receives an encrypted program in which a program is decrypted using a received key and then re-encrypted using at least some of the identification information.

Goodman et al. (US Pub. No. 2004/0230815 A1) teaches a system in which an upgrade is verified by the receiving machine accessing its unique identifier, a key

associated with the upgrade, process either identifier or the key, and compare to see if they match.

Ebert (US Pub. No. 2006/0064488 A1) teaches a software distributor which appends to a software application a hardware identification code.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JUSTIN MYHR whose telephone number is (571)270-7847. The examiner can normally be reached on Monday-Thursday 7:30 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dmitry Suhol can be reached on (571)272-4430. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JUSTIN MYHR/
Examiner, Art Unit 3714
7/28/2010

/Ronald Laneau/
Primary Examiner, Art Unit 3714